EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	322	726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/06/07 08:08
L2	386	713/188.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/06/07 08:09
L4	3	((thwart$4 or malicious) and attack and (data near2 center) and network and (separate or redundant) and traffic and monitor and dispersed and statist$4 and collect$4 and analyz$4).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/06/07 08:13
S1	2	"6321338".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/06/06 23:01
S2	2	"6775657".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/27 14:11
S3	2	"6591306".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 08:18
S4	1	09/931561	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 10:41
S5	97	(denial near service) same ((different or multiple or plurality or second) near2 (network or internet))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 10:42
S6	30	(denial near service) same (moniter$5 or detect$5) same ((different or multiple or plurality or second) near2 (network or internet))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 12:10

EAST Search History

S7	2	"6735702".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 12:10
S8	14	(attack) same (redundant network)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 13:01
S9	11	((denial near2 service) or ((malicious or trojan or virus) near2 attack)) same (redundant network)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 13:03
S10	40	((denial near2 service) or ((malicious or trojan or virus) near2 attack)) and (redundant network)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 13:53
S11	276	726/2.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 13:54
S12	516	726/22.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 14:00
S13	337	726/23.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 14:00
S14	250	726/24.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/04/28 14:00
S15	0	(control center).clm. and thwart$4. clm. and attack.clm. and physically. clm. and separate.clm. and monitor. clm. and analysis.clm. and malicious.clm. traffic.clm. filter$4. clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/13 19:30

EAST Search History

S16	0	(control center) and thwart$4 and attack and physically and separate and monitor and analysis and malicious traffic filter$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/13 19:32
S17	0	(control center) same thwart$4 same attack same physically same separate same monitor same analysis same malicious same traffic same filter$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/10/13 19:33

Terms used
thwart$4 or malicious and attack and data near2 center and network and separate or redundant and traffic and monitor and dispersed and statist$4 and collect$4 and analyz$4

Found 11,556 of 201,890

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next
Best 200 shown

Relevance scale

1 A holistic approach to service survivability
Angelos D. Keromytis, Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, Sal Stolfo
October 2003 **Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security SSRS '03**
Publisher: ACM Press
Full text available: pdf(1.58 MB) Additional Information: full citation, abstract, references, citings, index terms

We present SABER (Survivability Architecture: Block, Evade, React), a proposed survivability architecture that blocks, evades and reacts to a variety of attacks by using several security and survivability mechanisms in an automated and coordinated fashion. Contrary to the ad hoc manner in which contemporary survivable systems are built-using isolated, independent security mechanisms such as firewalls, intrusion detection systems and software sandboxes-SABER integrates several different techno ...

Keywords: intrusion detection, overlay networks, survivability

2 Protecting web servers from distributed denial of service attacks
Frank Kargl, Joern Maier, Michael Weber
April 2001 **Proceedings of the 10th international conference on World Wide Web WWW '01**
Publisher: ACM Press
Full text available: pdf(390.23 KB) Additional Information: full citation, references, citings, index terms

Keywords: DDoS, Linux, class based routing, distributed denial of service attacks, web server security

3 Scalable Networked Information Processing Environment (SNIPE)
Graham E Fagg, Keith Moore, Jack J Dongarra, Al Geist
November 1997 **Proceedings of the 1997 ACM/IEEE conference on Supercomputing (CDROM) Supercomputing '97**
Publisher: ACM Press
Full text available: pdf(77.42 KB) Additional Information: full citation, abstract, references, citings

SNIPE is a metacomputing system that aims to provide a reliable, secure, fault-tolerant environment for long-term distributed computing applications and data stores across the global InterNet. This system combines global naming and replication of both processing and data to support large scale information processing applications leading to better availablity and reliability than currently available with typical cluster computing and/or distributed computer environments.

Keywords: MetaComputing, RCDS, SNIPE, reliable, scalable, secure

4 Session summaries from the 17th symposium on operating systems principle (SOSP'99)
Jay Lepreau, Eric Eide
April 2000 **ACM SIGOPS Operating Systems Review**, Volume 34 Issue 2
Publisher: ACM Press
Full text available: Additional Information:

pdf(3.15 MB) full citation, index terms

5 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

6 The consensus problem in fault-tolerant computing
Michael Barborak, Anton Dahbura, Minoslaw Malek
June 1993 **ACM Computing Surveys (CSUR)**, Volume 25 Issue 2
Publisher: ACM Press
Full text available: pdf(4.60 MB) Additional Information: full citation, references, citings, index terms

Keywords: Byzantine agreement, consensus problem, decision theory, processor membership, system diagnosis

7 Security: LIGER: implementing efficient hybrid security mechanisms for heterogeneous sensor networks
Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, Thomas La Porta
June 2006 **Proceedings of the 4th international conference on Mobile systems, applications and services MobiSys 2006**
Publisher: ACM Press
Full text available: pdf(592.00 KB) Additional Information: full citation, abstract, references, index terms

The majority of security schemes available for sensor networks assume deployment in areas without access to a wired infrastructure. More specifically, nodes in these networks are unable to leverage key distribution centers (KDCs) to assist them with key management. In networks with a heterogeneous mix of nodes, however, it is not unrealistic to assume that some more powerful nodes have at least intermittent contact with a backbone network. For instance, an air-deployed battlefield network may ha ...

Keywords: heterogeneous sensor networks, hybrid network security, probabilistic authentication, probabilistic key management

8 Operating System Structures to Support Security and Reliable Software
Theodore A. Linden
December 1976 **ACM Computing Surveys (CSUR)**, Volume 8 Issue 4
Publisher: ACM Press
Full text available: pdf(3.49 MB) Additional Information: full citation, references, citings, index terms

9 Mining anomalies using traffic feature distributions
Anukool Lakhina, Mark Crovella, Christophe Diot
August 2005 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '05**, Volume 35 Issue 4
Publisher: ACM Press
Full text available: pdf(323.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The increasing practicality of large-scale flow capture makes it possible to conceive of traffic analysis methods that detect and identify a large and diverse set of anomalies. However the challenge of effectively analyzing this massive data source for anomaly diagnosis is as yet unmet. We argue that the distributions of packet features (IP addresses and ports) observed in flow traces reveals both the presence and the structure of a wide range of anomalies. Using entropy as a summarization tool, ...

Keywords: anomaly classification, anomaly detection, network-wide traffic analysis

10 Special issue on wireless pan & sensor networks: Design and analysis of Hybrid Indirect Transmissions (HIT) for data gathering in wireless micro sensor networks

Benjamin J. Culpepper, Lan Dung, Melody Moh

January 2004 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 8 Issue 1

Publisher: ACM Press

Full text available: pdf(440.82 KB) Additional Information: full citation, abstract, references, citings

Sensor networks have many potential applications in biology, physics, medicine, and the military. One major challenge in sensor networks is to maximize network life under the constraint of limited power supply. The paper addresses energy-efficiency in the context of routing and data gathering. A new protocol is proposed: Hybrid Indirect Transmission (HIT). HIT is based on a hybrid architecture that consists of one or more clusters, each of which is based on multiple, multi-hop indirect transmiss ...

11 Survey of network-based defense mechanisms countering the DoS and DDoS problems

Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao

April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1

Publisher: ACM Press

Full text available: pdf(1.17 MB) Additional Information: full citation, abstract, references, index terms

This article presents a survey of denial of service attacks and the methods that have been proposed for defense against these attacks. In this survey, we analyze the design decisions in the Internet that have created the potential for denial of service attacks. We review the state-of-art mechanisms for defending against denial of service attacks, compare the strengths and weaknesses of each proposal, and discuss potential countermeasures against each defense mechanism. We conclude by highligh ...

Keywords: Botnet, DDoS, DNS reflector attack, DoS, IP spoofing, IP traceback, IRC, Internet security, SYN flood, VoIP security, bandwidth attack, resource management

12 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2

Publisher: ACM Press

Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

13 The relational model for database management: version 2

E. F. Codd

January 1990 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(28.61 MB) Additional Information: full citation, abstract, references, citings, index terms, review

From the Preface (See Front Matter for full Preface)

An important adjunct to precision is a sound theoretical foundation. The relational model is solidly based on two parts of mathematics: firstorder predicate logic and the theory of relations. This book, however, does not dwell on the theoretical foundations, but rather on all the features of the relational model that I now perceive as important for database users, and therefore for DBMS vendors. My perceptions result from 20 y ...

14 Measurement: Automatically inferring patterns of resource consumption in network traffic

Cristian Estan, Stefan Savage, George Varghese

August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '03**

Publisher: ACM Press

Full text available: pdf(260.43 KB) Additional Information: full citation, abstract, references, citings, index terms

The Internet service model emphasizes flexibility -- any node can send any type of traffic at any time. While this design has allowed new applications and usage models to flourish, it also makes the job of network management significantly more challenging. This paper describes a new method of traffic characterization that automatically groups traffic into minimal clusters of conspicuous consumption. Rather than providing a static analysis specialized to capture flows, applications, or network-to ...

Keywords: data mining, network monitoring, traffic measurement

15 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

16 Illustrative risks to the public in the use of computer systems and related technology

Peter G. Neumann

January 1996 **ACM SIGSOFT Software Engineering Notes**, Volume 21 Issue 1

Publisher: ACM Press

Full text available: pdf(2.54 MB) Additional Information: full citation

17 Technical papers: Imaging and visual analysis---Detecting distributed scans using high-performance query-driven visualization

Kurt Stockinger, E. Wes Bethel, Scott Campbell, Eli Dart, Kesheng Wu

November 2006 **Proceedings of the 2006 ACM/IEEE conference on Supercomputing SC '06**

Publisher: ACM Press

Full text available: pdf(433.00 KB) html(2.35 KB) Additional Information: full citation, abstract, references

Modern forensic analytics applications, like network traffic analysis, perform high-performance hypothesis testing, knowledge discovery and data mining on very large datasets. One essential strategy to reduce the time required for these operations is to select only the most relevant data records for a given computation. In this paper, we present a set of parallel algorithms that demonstrate how an efficient selection mechanism -- bitmap indexing -- significantly speeds up a common analysis task, ...

Keywords: data mining, network connection analysis, network security, query-driven visualization, visual analytics

18 Internet traffic classification using bayesian analysis techniques

Andrew W. Moore, Denis Zuev

June 2005 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems SIGMETRICS '05**, Volume 33 Issue 1

Publisher: ACM Press

Full text available: pdf(698.73 KB) Additional Information: full citation, abstract, references, citings, index terms

Accurate traffic classification is of fundamental importance to numerous other network activities, from security monitoring to accounting, and from Quality of Service to providing operators with useful forecasts for long-term provisioning. We apply a Naïve Bayes estimator to categorize traffic by application. Uniquely, our work capitalizes on hand-classified network data, using it as input to a supervised Naïve Bayes estimator. In this paper we illustrate the high level of accuracy ach ...

Keywords: flow classification, internet traffic, traffic identification

19 Defeating DDoS attacks by fixing the incentive chain

Yun Huang, Xianjun Geng, Andrew B. Whinston

February 2007 **ACM Transactions on Internet Technology (TOIT)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(1.99 MB) Additional Information: full citation, abstract, references, index terms

Cooperative technological solutions for Distributed Denial-of-Service (DDoS) attacks are already available, yet organizations in the best position to implement them lack incentive to do so, and the victims of DDoS attacks cannot find effective methods to motivate them. In this article we discuss two components of the technological solutions to DDoS attacks: cooperative filtering and cooperative traffic smoothing by caching. We then analyze the broken incentive chain in each of these technologica ...

Keywords: Denial-of-service, incentive, pricing, security

20 Miscellaneous I: A wavelet-based framework for proactive detection of network misconfigurations

Antonio Magnaghi, Takeo Hamada, Tsuneo Katsuyama

September 2004 **Proceedings of the ACM SIGCOMM workshop on Network troubleshooting: research, theory and operations practice meet malfunctioning reality NetT '04**

Publisher: ACM Press

Full text available: pdf(263.62 KB) Additional Information: full citation, abstract, references, index terms

An increasing number of misconfigurations and malicious behaviors threaten the normal operation conditions of data networks. Thus, field engineers are constantly presented with the challenge of isolating new misconfigurations and anomalies. In this paper, we present a group of real-world problems reported by a set of six commercial networks we surveyed. Successively, we focus on a well-defined family of misconfigurations. Our analysis identifies common properties such anomalous behaviors share. ...

Keywords: misconfiguration, network performance, retransmissions, wavelets

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next